IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
MIDLAND-ODESSA DIVISION

MALIKIE INNOVATIONS LTD., KEY PATENT INNOVATIONS LTD. Plaintiffs, v. MARA HOLDINGS, INC. (F/K/A MARATHON DIGITAL HOLDINGS, INC) Defendant.	CASE NO. 7:25-cv-00222-DC-DTG JURY TRIAL DEMANDED

MARA'S REPLY CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

I. INTRODUCTION

The intrinsic and extrinsic record supports MARA Holdings, Inc.'s ("MARA") constructions of the disputed terms. Malikie Innovations Ltd.'s ("Malikie") positions lack merit and should be rejected for the reasons explained below.

II. ARGUMENT

A. The '286 Patent

1. "Montgomery-style reduction"

MARA's Construction	Malikie's Construction
"reduction that proceeds by clearing the least significant portions of an unreduced operand and leaving the remainder in the more significant portions"	This term appears only in the preamble and is not limiting. Should the Court find this term is limiting, it should be construed to mean: "reduction that proceeds by clearing the least significant portions of an unreduced quantity, leaving the remainder in the more significant portions."

First, Malikie argues the preamble is not limiting because "the body of the claim itself…(without any need for the preamble) is what defines the particular 'alternative way'…of conducting a Montgomery reduction." Dkt. 53 at 5. Yet, Malikie and its expert interpret the body of the claim to encompass reduction methods far beyond alternative ways of conducting Montgomery reduction. Dkt. 52 at 11; Dkt. 52-2 at ¶ 58-64. Malikie cannot have it both ways—it cannot contend that the claim body defines "an 'alternative way' of conducting Montgomery reduction" (Dkt. 53 at 5), but then assert that those very same steps cover other types of reduction (including prior art methods) having nothing to do with Montgomery reduction. Here, the singular focus of the '286 Patent is Montgomery-style reduction. Dkt. 52 at 10; Dkt. 52-3 at 1:13-16, 3:20-26. The Court should reject Malikie's attempt to untether the claim from this focus. The preamble is limiting because it "provides essential context to properly understand the body of the claim." *UNILOC 2017 LLC* v. *Verizon Comm'n, Inc.*, 2020 WL 805271, at *11 (E.D. Tex. Feb. 18, 2020).

Second, Malikie relies on the Federal Circuit's decision in *Arctic Cat* to argue that the preamble language "personal recreational vehicle" was "entirely conventional apart from the improvement in the body of the claims," and contends that, as in *Arctic Cat*, "the novelty of the invention in Claim 1 [of the '286 Patent] is captured in the recited elements of the claim." Dkt. 53 at 5-6 (citing *Arctic Cat Inc.* v. *GEP Power Prods., Inc.*, 919 F.3d 1320, 1327 (2019)). Malikie's reliance is misplaced. Malikie ***does not rebut*** that under its proposed interpretation, the claim covers the prior art pseudo-Mersenne reduction. It is therefore undisputed that the purported novelty of claim 1 is ***not*** captured by the body of the claim under Malikie's proposed interpretation. Furthermore, Malikie is mistaken that MARA argues the preamble is limiting "to avoid the alleged prior art." As explained in MARA's opening brief, that the claim reads on prior art pseudo-Mersenne reduction under Malikie's proposed interpretation demonstrates that Malikie is "read[ing] the claim indiscriminately to cover all types of [reduction] [which is] divorced from reality." *GE Co.* v. *Nintendo Co.*, 179 F.3d 1350, 1361 (Fed. Cir. 1999).

Third, Malikie contends that the preamble is not limiting because "Montgomery-style reduction" merely recites an intended use or purpose for the claimed method. Not so. The preamble describes ***how*** the method must proceed—by reducing from below *instead* of reducing from above. Here, "review of the entirety of the [specification] reveals that the preamble language relating to [Montgomery-style reduction] does not state a purpose or intended use of the invention, but rather discloses a ***fundamental characteristic of the claimed invention*** that is properly construed as a limitation of the claim itself." *Poly-Am., L.P.* v. *GSE Lining Tech., Inc.*, 383 F.3d 1303, 1310 (Fed. Cir. 2004) (emphasis added).

Finally, Malikie objects that MARA's construction of the preamble, which uses the phrase "unreduced operand" should be rejected in favor of Malikie's proposal that uses the phrase

"unreduced quantity," because MARA is reading out preferred embodiments involving performing multiple iterations of an operation on previously or partially reduced operands. Dkt. 53 at 7. But there is no difference between "operand" and "quantity" that would lead the former to read out embodiments, but not the latter. Neither construction reads out an embodiment. Indeed, it cannot seriously be disputed that the term "operand" includes "quantities." Malikie's expert confirmed this during deposition. When asked to explain the difference, Malikie's expert evaded the question. Ex. B at 76:1-78:25. He conceded that an "operand" is a number, but took the incredible position that it would be too confusing to answer whether an "operand" is a quantity. *Id*. As explained in MARA's Opening Brief, the Court should adopt MARA's construction because the claims require that the "operand" is the unreduced quantity on which the reduction proceeds. Dkt. 52 at 11.

Therefore, the Court should find the preamble limiting and adopt MARA's construction.

2. "perform a replacement of a least significant word of the operand"

MARA's Construction	Malikie's Construction
"add a modular equivalent of the operand's least significant word to the more significant words of the operand such that the result can be shifted down to drop the least significant word"	"replace a word that makes the smallest contribution to the value of the operand"

Malikie contends that "replacement" should have its plain and ordinary meaning such that "perform a replacement of a least significant word" means that "the least significant word of the operand is 'replaced' with another value." Dkt. 53-2 at ¶ 69. In other words, Malikie contends that "perform a replacement" does not require any construction, and disputes that it requires adding a modular equivalent of the least significant word ("LSW") as proposed by MARA. The Court should reject Malikie's superficial position for the reasons explained below.

First, it is undisputed that the claims are directed to ***reduction*** (i.e., calculation of a remainder). *See* Ex. B at 54:6-55:4 (Malikie's expert conceding that "reduction in this context is

calculation of a remainder."). As MARA's expert explained, in order to correctly calculate the remainder, "replacement" in the context of the '286 patent must involve adding a modular equivalent of the LSW. Dkt. 52-2 at ¶¶ 54-57. Malikie's "plain meaning" interpretation, however, allows adding *any value* that changes the LSW. But as explained below, using *any* value that changes the LSW would not result in ***reduction*** (i.e., calculation of a remainder). Specifically, MARA's opening brief provided an example showing how the '286 Patent method is used to correctly calculate 4355 mod 97, which equals 87. Dkt 52 at 7-8. In that example, the "replacement" (step 4) involves adding $T_0 \times n' \times 10^w$, which is a modular equivalent of the LSW. During deposition, Malikie's expert was shown a new example (Ex. C), reproduced below, which tracks the example in MARA's opening brief ***except*** that it adds a randomly selected number to replace the LSW instead of $T_0 \times n' \times 10^w$. Ex. B at 129:1-131:9.

<table>
<tr><td colspan="2">Assumptions: modulus n = 97; word-size = 2; a = 4355
Goal: calculate 4355 mod 97 (i.e., a mod n)
Answer: 4355 mod 97 = 87</td></tr>
<tr><td>1. Convert a to Montgomery form (T):
T = a × R mod n = 4355 × 10000 mod 97
T = 4355 x 10000 mod 97
T = 39195

2. Calculate n' = 10^{-w} mod n:
n' = 10^{-2} mod 97
n' = 65

3. Use n' to replace LSW with another value:
39195 + n' × 1952
39195 + 65 × 1952 = 166075</td><td>4. Shift T to the right by two digits:
166075 → 1660

Perform standard Montgomery red. on 1660

5. Calculate μ and m:
μ = (-n)-1 mod 10^w = (-97)-1 mod 100 = 67
m = μ×T_0 mod 10^w = 67×60 mod 100 = 20

6. Add m×n to T:
1660 + 20 × 97 = 3600

7. Shift T to the right by two digits:
3600 → 36</td></tr>
</table>

***See* Ex. C**

In step 3 of the new example, the value 65×1952 (126880) is added. Malikie's expert agreed that this accomplished "replacement" as Malikie construes the term because the LSW was changed from **95** to **75**. *Id.* at 131:10-25. Despite "performing a replacement of the least significant

word" as Malikie interprets the term, the example computes an ***incorrect*** result of 36. *Id.* at 132:1-13. The example illustrates that, to perform ***reduction***, it is not acceptable to add *any* value that changes the LSW. Instead, as Malikie's expert admitted, "it is important that you select a value for whatever reduction you're doing that is going to work properly with that reduction." Ex. B at 67:12-18; 132:1-24. Accordingly, Malikie's plain meaning construction is overbroad because it encompasses changing the LSW in a manner that will ***not*** perform reduction correctly.

Second, Malikie contends that MARA's construction limits the claim to the sole embodiment in the specification because it requires using a shifted version of n'. Dkt. 53 at 9-10. But both experts agree that MARA's construction does no such thing. Malikie's expert testified that he "do[es]n't think that the language in MARA's construction specifically is limited to using shifted reduction value," that "a shifted reduction value is one type of modular equivalent," and that "MARA's construction doesn't require specifically the use of a shifted reduction value for modular equivalence." Ex. B at 49:17-51:6. Consistently, Dr. Koc's deposition testimony and reply declaration describe multiple alternative ways to perform replacement under MARA's construction that are not limited to the sole embodiment in the specification. Dkt. 53-5 (Koc Dep. Tr.) at 59:20-61:18; Ex. A at ¶¶ 6-17. For example, the sole embodiment performs a replacement by adding the term $a_0 \times n' \times 2^w$. Dkt. 52-3 at 5:59-62. Dr. Koc's reply declaration shows using three different addends, each modularly equivalent to the LSW, to correctly perform reduction. Ex. A at ¶¶ 6-11. Additionally, the sole embodiment describes zeroing the LSW first and then adding $a_0 \times n' \times 2^w$. Dkt. 52-3 at 5:59-62. Dr. Koc demonstrates that alternatively, replacement can be done by first adding $a_0 \times n' \times 2^w$ and then zeroing the LSW, or not zeroing at all. *Id.* at ¶¶ 12-17. Each example is within the scope of MARA's construction and correctly calculates the remainder. *Id.* at ¶¶ 6-17. Thus, MARA's construction is not limited to the sole embodiment.

Third, Malikie's inconsistent positions regarding the claim terms "perform a replacement" and "perform a cancellation" cannot be reconciled. On the one hand, Malikie contends that, in the context of the '286 Patent, the term "perform a cancellation" means something more specific than the "ordinary sense" of cancellation. Specifically, Malikie's expert explained that the "ordinary sense" of cancellation means "to eliminate" (Dkt. 53-2 at ¶ 77), but nonetheless admits that "[t]he phrase perform a cancellation thereof is talking about eliminating ***by doing something specific—something more specific***." Ex. B at 84:3-22. Indeed, the parties agree in their constructions that the "something more specific" in this context is "adding a multiple of the modulus to the operand." Yet, Malikie takes the inconsistent position that "perform a replacement" requires "replaced in the ordinary sense" and nothing more specific. Dkt. 53-2 at ¶ 70; Dkt. 53 at 8. Malikie has no explanation for its contrary position, and as explained above, its overly broad position regarding "replacement" is mathematically incorrect because it encompasses changing the LSW in a manner that does not correctly calculate reduction. The consistent position, set forth by MARA, is that both terms require "something more specific" in this context.

3. "perform a cancellation thereof"

MARA's Construction	Malikie's Construction
"add a multiple of the modulus to the operand such that the least significant word of the result is zero and the result can be shifted down to drop the least significant word"	"add a multiple of the modulus to the operand to eliminate the least significant word of the operand"

The parties agree that, in the context of the '286 Patent, "perform a cancellation thereof" means something more than the ordinary sense of "cancellation" and requires adding a multiple of the modulus to "zero" the LSW of the operand. Dkt. 53 at 11. The parties also agree that, once zeroed, the LSW should be dropped.

Despite agreeing that adding a multiple of the modulus zeroes the LSW, and then the zeroed LSW is dropped, Malikie's construction attempts to capture these specific steps by using the vague term "eliminate." The Court should adopt MARA's construction because it provides greater precision regarding the particular steps required to perform a cancellation. Furthermore, it appears from the deposition of Malikie's expert that Malikie believes that the LSW is dropped by shifting or truncating. Ex. B at 89:22-90:24. To the extent Malikie believes the proper construction should require shifting or truncating to drop the zeroed LSW, MARA does not object.

B. The '062 and '960 Patents

1. "finite field operation"

MARA's Construction	Malikie's Construction
"operation where each operand is a finite field element"	"operation in a finite field"

The dispute regarding this term is clear— Malikie contends that the finite field operations include operations on elliptic curve points (Dkt. 53 at 13); MARA contends that finite field operations are limited to operations on finite field elements (Dkt. 52 at 17). Malikie is wrong because the specification is clear that finite field operations are operations on finite field elements, not elliptic curve points.

It is undisputed that "an elliptic curve point consists of two finite field elements." Dkt. 52-4 at 7:27-28; Dkt 52-2 at ¶ 68. But this does not mean that an elliptic curve point is a finite field element, or vice versa. Nor does it mean that finite field operations are operations on elliptic curve points. Indeed, the specification clearly distinguishes between elliptic curve operations and finite field operations. Dkt. 52-4 at 6:61-66 ("The implementation of the protocol 210 requires the use of both elliptic curve operations and finite field operations."); *see also* Dkt. 52-2 at ¶ 67. For example, elliptic curve point addition operates on two elliptic curve points (e.g., P and Q) and outputs a third point (e.g., R), and can be geometrically described as calculating where a line

through points P and Q intersects the curve, and obtaining a third point R where the intersection reflects across the x-axis. Dkt 52-2 at ¶ 68. In contrast, finite field addition is a completely different operation involving the arithmetic addition of two finite field elements and reducing the result to the finite field (i.e., a + b mod n). *Id*.

It is also undisputed that elliptic curve operations involve conducting finite field operations. Dkt. 52-4 at 7:26-27 ("Each elliptic curve operation 320 requires certain finite field operations."). But the fact that an elliptic curve operation requires performing certain finite field operations does not make a finite field operation an operation on elliptic curve points. Rather, the specification is unambiguous that finite field elements are only operated on by the finite field engine that carries out finite field operations. Dkt. 52-4 at 7:28-29 ("The finite field elements are ***only operated on directly*** in the finite field engine 400"), 8:26-27 ("The finite field engine 400 provides finite field routines 430 for use by the cryptographic engine 200 and the elliptic curve engine 300"). Moreover, the examples in the specification confirm that finite field operations involve operating on finite field elements, not elliptic curve points. Dkt. 52-4 at 8:26-29, 9:8-12, 10:12-19.

A finite field operation is unquestionably an operation on finite field elements, not an operation on finite field elements *and* elliptic curve points. The claims at issue are specifically directed to a "finite field operation," not to an elliptic curve operation. Thus, Malikie's attempt to broaden the claims to encompass both should be rejected.

2. "unreduced result"

MARA's Construction	Malikie's Construction
"result without any reduction to a specific finite field or wordsize reduction"	"result without performing the claimed modular reduction"

After reviewing MARA's opening brief, Malikie realized the fundamental errors in its initial construction of "unreduced result." But its revised construction fares no better. While

Malikie's revised construction correctly identifies that an unreduced result cannot have been obtained by performing modular reduction, it is incorrect because it permits an unreduced result to be a result that is obtained by performing a wordsize reduction.

Critically, the specification identifies two types of reduction—"reduction may be specific to a certain finite field [i.e., modular reduction], or a wordsize reduction." Dkt. 52-4 at 8:51-54; *see also* Dkt. 52-2 at ¶¶ 73-74. Neither Malikie nor its expert addresses the two types of reduction disclosed in the specification. Indeed, at his deposition, despite having read and cited the critical portion of the '960 Patent, Malikie's expert conceded that he had no opinion regarding the two types of reduction disclosed and was unable to testify as to the difference between the two. Ex. B at 97:2-98:17, 100:5-12, 104:7-16. Because the specification identifies that a result may be reduced in either way, it follows that an "unreduced result" is one that is not reduced in either way. But under Malikie's construction, a result that was obtained by performing a wordsize reduction would incorrectly fall within the scope of "unreduced result," contrary to the specification.

Malikie further errs by contending that "the claim already states what type of reduction is *not* performed on an unreduced result, i.e., modular reduction." Dkt. 53 at 18. This is false. The claims state what type of reduction *is* performed to obtain a reduced result (i.e., reduction specific to a certain finite field). Dkt. 52-4, claim 3 ("performing a specific modular reduction of said unreduced result to reduce said unreduced result to that of a field element of said finite field to obtain a reduced result"); Dkt. 52-5, claim 1 ("performing a modular reduction for a specific finite field…to generate a reduced result"). But the claims are silent as to what types of reduction are not performed to obtain an unreduced result. Dkt. 52-4, claim 3 ("completing said non-reducing wordsized operation for each word of said representations to obtain an unreduced result"); Dkt. 52-5, claim 1 ("executing the first set of instructions to generate an unreduced result completing

the finite field operation"). It is undisputed that there are two types of reduction, and therefore, without any other clarification in the claim, the term "unreduced result" means without performing either type of reduction—i.e., "without any reduction to a specific finite field or wordsized reduction." Accordingly, MARA's proposed construction should be adopted.

3. "reduced result"

MARA's Construction	Malikie's Construction
No construction needed. Plain and ordinary meaning.	"result of performing the claimed modular reduction"

This term requires no construction because the claim language plainly states what is performed to obtain a reduced result—"a specific modular reduction" (Dkt. 52-4, claim 3) / "a modular reduction for a specific finite field" (Dkt. 52-5, claim 1). Malikie recognized that its original proposed construction ("result of an operation whose bit length has been lowered") was erroneous, and now proposes that the term be construed as "result of performing the ***claimed*** modular reduction." Because this revision merely refers back to the claim, Malikie in effect concedes that no construction is needed. The Court should not adopt Malikie's circular construction as it does not provide any further guidance beyond what is claimed.

C. The '827 and '370 Patents

1. "the electronic message omits a public key of a signer" ['370]

MARA's Construction	Malikie's Construction
"the electronic message does not include any representation of the public key of the signer"	Plain and ordinary meaning

First, Malikie claims that MARA "does not explain what [] 'any representation of' means." Dkt. 53 at 21. MARA, however, clearly explained a "representation of the public key Q" is a form of the public key Q (e.g., a compressed version of Q) "such that the public key Q could be obtained from the representation [without] need to recover the public key Q ***using the specific equation recited in the claim***." Dkt. 52 at 25. Interpreting the claim to allow (rather than omit) sending such

a representation of the public key Q would render the claimed recovery equation pointless. Malikie notes that the specification expressly teaches an embodiment that involves sending "a compact version of Q…***instead*** of Q." Dkt. 53 at 21 (citing Dkt. 52-7 at 16:22-27). This embodiment is not relevant to the claims, which are directed to recovering the public key Q using a specific recovery equation. Indeed, sending a representation of the public key Q from which the public key Q could be determined without the recovery equation would render the recovery equation unnecessary.

Second, Malikie contends that MARA's construction "would read out every embodiment of the invention" because it would require omitting the signature (r,s). This interpretation is nonsensical. The claim language explicitly states that the signature (r,s) is sent with the message, and therefore, cannot be omitted. The signature (r,s) is not a representation of the public key Q. Moreover, the claimed recovery equation computes Q using the signature (r,s). Thus, sending the signature (r,s) facilitates the public key recovery operation; it does not render it unnecessary.

Third, Malikie claims that the applicant's arguments during the prosecution history discussed in MARA's opening brief (Dkt. 52 at 25-26) are inapplicable because of a subsequent amendment to the claims replacing "***any*** public key" with "***a*** public key." Dkt. 53 at 22-23. MARA disagrees. The pending claim at the time of the applicant's statements recited omitting "***any public key*** of a signer," not ***all public keys***, as Malikie's argument suggests. Dkt. 53 at 22. Thus, there is no evidence that the applicant considered the short term public key disclosed in Gallant to be a separate, "un-omitted" public key to the second elliptic curve point Q.[1] *Id.*

Accordingly, the Court should adopt MARA's proposed construction.

[1] Malikie also states that "indeed, the claims did not refer to Q then." Dkt. 53 at 22. But the then-pending claims did refer to "the public key compris[ing] a second elliptic curve point," (*i.e.*, Q). Dkt. 53-7 at 4595.

2. "verifying that the second elliptic curve point Q represents the public key of the signer" ['827]

MARA's Construction	Malikie's Construction
"verifying that the second elliptic curve point Q represents the second elliptic curve point Q"	Plain and ordinary meaning

Malikie does not dispute that the antecedent basis for both "the second elliptic curve point Q" and "the public key of the signer" in claim 2 is the value Q that is computed using the equation $Q = r^{-1}(sR - eG)$. Dkt. 53 at 23-24. Thus, Malikie admits that MARA's construction aligns exactly with the claim language—i.e., both the "second elliptic curve point" and "the public key of the signer" are the value Q that is computed. While Malikie cites a portion of the specification that describes comparing the computed Q to the actual public key of the signer (i.e., a public key of the signer that is received from the signer or looked up in a database), that is not what is recited in claim 2. Dkt. 53 at 23. Malikie cites no case law that would allow the Court to redraft the claim.

Accordingly, the Court should adopt MARA's proposed construction.

D. The '961 Patent

1. "random number generator"

MARA's Construction	Malikie's Construction
"a system or algorithm that generates a random value"	"computer instructions capable of generating values according to a uniform random probability distribution"

A "random number generator" (RNG) ***in the context of cryptography*** refers to a system or algorithm that generates a ***random*** value, as distinct from pseudorandom number generators that generate deterministic values. Malikie's arguments that broaden the scope of an RNG beyond its plain meaning in the context of the claims (*i.e.*, cryptographic functions) should be rejected.

First, Malikie's assertion that the specification recites the meaning of RNG by stating that RNGs select values with "a uniform distribution throughout the defined interval" is incorrect. *See*

Dkt. 53 at 25 (citing Dkt. 52-8 at 2:15-17, 2:29-32). While generating values with a "uniform distribution throughout the defined interval" is a property of an RNG in cryptography, it is not the only property. Both parties' experts agree that an RNG in cryptography must also generate unpredictable values. Dkt. 53-5 at 103:13-20 ("for cryptography, not only do they have to be uniformly distributed, but they also have to be ***unpredictable***."); Ex. B at 117:24-119:8; Dkt. 53-8 at 398 ("The term ***random numbers***…includes pseudorandom numbers ***which are unpredictable***…."). Both experts also agree that deterministic PRNGs are not suitable for cryptography, because they are predictable. Dkt. 53-5 at 92:5-22; Ex. B at 119:1-17. Malikie's construction is overbroad because it does not require unpredictable values, which is a required property of RNGs in cryptography.

Second, the relevant extrinsic evidence cited by Malikie supports MARA's position. Malikie cites the Handbook of Applied Cryptography ("Handbook") to support its position that "random numbers" need only have uniform distribution. Dkt. 53-8 at 398. The cited excerpt, however, also states that "random numbers" in the context of cryptography only include "pseudorandom numbers ***which are unpredictable***." *Id*. Thus, the Handbook confirms that MARA's construction is correct because it explains that RNGs in cryptography output values that are actually random (*i.e.* non-deterministic). *See also* Dkt. 52-2 at ¶¶ 84-87 (explaining that RNGs in cryptography produce actually random values).

Third, MARA did not argue that DSS excludes PRNGs, as Malikie contends. Dkt. 53 at 29. Rather, DSS demonstrates that a POSITA would have understood that "random" and "pseudorandom" numbers are different in cryptography, and one would not interpret "random" to encompass all "pseudorandom" values. Dkt. 52-17 at 2068, 2075; Dkt. 52-2 at ¶ 86.

Fourth, the definitions of "random" and RNG that Malikie cites should be given no weight. The "specialized computer and computer science dictionaries" that Malikie relies on (Dkt. 53 at 28) are irrelevant because they define RNG in the context of general computing, not the specific field of the '961 patent (*i.e.*, cryptography). *See, e.g.*, Dkt. 52-8 at 3:1-3; *Teva Pharms. USA, Inc.* v. *Sandoz, Inc.,* 574 U.S. 318, 331 (2015) (extrinsic evidence can inform the meaning of a term "in ***the relevant art*** during the relevant time period."). As explained in MARA's opening brief, "randomness" in the context of cryptography "differs from randomness in the traditional statistical sense," and does not include deterministic values. Dkt. 53-8 at 398; *see also* Dkt. 52-20 at 77, 81 (using "random" to refer to "pseudorandom number generators" is a "slight abuse of language").

The cases Malikie cites construing the term "random" are similarly inapposite. The patent in *Northeastern University* v. *Google, Inc.*, 2010 WL 4511010, at *1 (E.D. Tex. Nov. 9, 2010), was directed to "search database architecture," while the patents in *Inst. of Tech.* v. *Broadcom Ltd.*, 2019 WL 11828243, at *4 (C.D. Cal. Nov. 25, 2019), were directed to a forward error correction technique in communications systems. Neither defined "random" in cryptography.

Fifth, Dr. Koc did not admit that deterministic RNGs or PRNGs fall within the scope of an RNG in cryptography, as Malikie contends. Dkt. 53 at 28. Dr. Koc explained that "RNG" is used in his textbook as a "general name" that "includes everything," but RNG has a "very specific" meaning in cryptography. Dkt. 53-5 at 91:24-92:1. Dr. Koc further explained that RNGs in cryptography refer to systems incorporating some "physically or naturally occurring source of randomness that has higher entropy included," including "cryptographically-secure PRNGs" using a physical entropy seed. *Id.* 92:1-5, 94:24-95:6. "PRNGs, ***without any physical randomness injected***, would not be suitable for cryptography," and thus not considered an RNG. *Id.* at 92:1-7. Dr. Koc's textbook is consistent with his testimony, stating that a "necessary requirement" for

RNGs in "cryptographic applications" is unpredictability—"the knowledge of subsequences of random numbers shall not allow one to *practically* compute predecessors or successors or to guess these numbers…." Dkt. 53-13 at 6; *see also* Dkt. 52-2 at ¶¶ 85-87.

Accordingly, the Court should adopt MARA's proposed construction

2. "seed"

MARA's Construction	Malikie's Construction
"a random value that is used as the starting value for a cryptographic key generation function"	"a value obtained from a random number generator that is used as the starting value for a cryptographic key generation function"

Malikie principally argues that because an RNG need not output random values, a seed value is not random in the context of the '961 Patent. *See* Dkt. 53 at 31-32. Malikie is incorrect.

First, Malikie does not dispute that the prior patent owners represented that the "seed value" of claim 1 is "random" during prosecution and the subsequent IPR to avoid prior art. Dkt. 52 at 30-31; Dkt. 52-18 at 41-42, 46, 47, 48. Malikie attempts to sidestep these admissions by asserting that the term "random" during prosecution was intended to encompass pseudorandom as well. Dkt. 53 at 32, n. 17. This is incorrect. In response to a rejection under §102(b) during prosecution, the applicant distinguished prior art relating to DSS by asserting that the value k in DSS "is not an output that is a result of a hash on a seed number chosen at random, ***it is a random number in itself***." *Id.* In other words, the applicant differentiated between (1) performing a deterministic hash function on a seed (*i.e.*, a PRNG)[2]; and (2) a random number *in itself.* The prosecution history thus demonstrates that the applicant used the term "random" to refer to values that are actually random, which differ from deterministic pseudorandom values.[3]

[2] Performing a hash on a seed is an implementation of a PRNG. Ex. B at 121:8-21.

[3] The distinction is also evident from the use of "deterministic" in claim 7, in contrast to the use of "random" in claim 1.

Second, extrinsic evidence confirms that a "seed value" in the context of cryptography is random. While Malikie cites several dictionary definitions to support its position, those definitions are irrelevant because they do not define "seed" in cryptography. Dkt. 53 at 31 (citing Ex. 8 and Ex. 11). Both experts agree that a cryptographic seed value must be generated via entropy (*i.e.*, it is random and not deterministic). Dkt. 52-2, ¶ 87; Ex. B at 121:23-122:4. The expert testimony is consistent with the Handbook, explaining that for cryptographic applications "***an initial seed with sufficient entropy is required***." Dkt. 53-8 at 399. In contrast, Malikie identified no evidence that a "seed value" in a cryptographic function can be deterministic.

Accordingly, the Court should adopt MARA's proposed construction.

3. Claim 7 is Indefinite

Claim 7 is indefinite because a POSITA would not understand with reasonable certainty how to perform the steps of claim 7 in combination with "repeating said method" of claim 1 after "output H(SV)" is rejected. Malikie's position—that the steps in claim 7 comprise one of multiple ways of "repeating said method" of claim 1—is inconsistent with the claim language, untethered from the specification, and defies well-settled claim interpretation principles. Dkt. 53 at 33-34.

Claim 1 recites a "method" of generating a key k, which requires the steps of, *inter alia*, (a) generating a seed value SV, (b) performing a hash function on SV to provide an output H(SV), and (c) determining whether output H(SV) is less than order q. Claim 1 further requires that if "output H(SV) is rejected, repeating said method." Malikie's expert conceded that "repeating said method" in claim 1 clearly requires repeating steps (a)-(c) above. Ex. B at 123:16-25. Nevertheless, Malikie's responsive brief contends that "repeating said method" in claim 1 does not require repeating steps (a)-(c), but instead encompasses "multiple ways of performing said method," including the steps in claim 7. Dkt. 53 at 33; Ex. B at 125:25-126:25 (Malikie's expert asserting that incrementing a rejected output constitutes generating a seed value from an RNG). Malikie's

interpretation of claim 1 is nonsensical under any reasonable definition of "repeating" and cannot save claim 7 from indefiniteness.

The specification also confirms that Malikie's interpretation is incorrect. Notably, the specification never describes the steps in claim 7 as a variant that falls within the scope of generating a new seed value from an RNG and performing a hash thereon after a rejection (*i.e.*, repeating said method of claim 1), as Malikie contends. To the contrary, the specification clearly describes (1) generating a seed value from an RNG and (2) incrementing a prior value as separate and distinct steps performed in different methods. Dkt. 52-8 at 4:50-52 ("Upon rejection, the random number generator may generate a new value…***or*** may increment the seed value….").

As explained in MARA's opening brief, the plain language of claims 1 and 7 require that if output H(SV) is rejected, "said method" is repeated (*i.e.*, steps (a)-(c) of claim 1 are repeated) ***and*** the additional steps of claim 7 are performed. Dkt. 52 at 33-35. The '961 Patent, however, fails to describe with reasonable certainty how to repeat "said method" in combination with performing claim 7's steps, which Malikie does not dispute. Accordingly, claim 7 is indefinite.

Finally, MARA has not argued that claim 7 is indefinite because it may be interpreted in multiple ways, as Malikie contends. *See* Dkt. 53 at 34, n. 19. MARA has asserted that claim 7 is indefinite because it fails to provide a POSITA with reasonable certainty regarding how to perform the two different sets of steps from claims 1 and 7 together if output H(SV) is rejected. Dkt. 52 at 34. Malikie's inability to do so confirms that MARA's position is correct.

III. CONCLUSION

For the reasons set forth herein and in MARA's opening claim construction brief, the Court should adopt MARA's proposed claim constructions.

Dated: January 28, 2026

Respectfully Submitted,

PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP

/s/ Anish Desai
Anish Desai
Elizabeth S. Weiswasser
Ian A. Moore
Tom Yu
Thomas Macchio
Paul, Weiss, Rifkind, Wharton & Garrison LLP
1285 Sixth Avenue
New York, NY 10019
Telephone: (212) 373-3000

Christopher M. Pepe
Priyata Patel
W. Sutton Ansley
Eric C. Westerhold
Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K Street NW
Washington, DC 20006
Telephone: (202) 223-7300

Steve Wingard
State Bar No. 00788694
swingard@scottdoug.com
Robert P. Earle
State Bar No. 241245566
rearle@scottdoug.com
Stephen L. Burbank
State Bar No. 24109672
sburbank@scottdoug.com
Scott Douglass & McConnico LLP
303 Colorado Street, Suite 2400
Austin, TX 78701-3234
Telephone: (512) 495-6300
Facsimile: (512) 495-6399

Counsel for Defendant MARA Holdings, Inc.

CERTIFICATE OF SERVICE

The undersigned attorney hereby certifies that on January 28, 2026, I caused correct copies of the foregoing document to be served via email on all counsel of record.

/s/ Anish Desai
Anish Desai